

(19) 日本国特許庁 (JP)

# (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2 0 0 2 - 8 2 9 1 1

(P 2 0 0 2 - 8 2 9 1 1 A)

(43) 公開日 平成14年3月22日 (2002. 3. 22)

(51) Int. Cl. <sup>7</sup>	識別記号	F I	テーマコード (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 C 5B035
			3 3 0 G 5B058
	Z E C		Z E C 5B085
G 0 6 K 17/00		G 0 6 K 17/00	L 5J104
19/10		19/00	R
審査請求 有	請求項の数 7	O L	(全 6 頁) 最終頁に続く

(21) 出願番号 特願2000-274421 (P2000-274421)

(22) 出願日 平成12年9月11日 (2000. 9. 11)

(71) 出願人 000004237  
日本電気株式会社  
東京都港区芝五丁目7番1号

(72) 発明者 諏訪本 剛  
東京都港区芝五丁目7番1号 日本電気株式  
会社内

(72) 発明者 大沢 一秋  
東京都港区芝五丁目7番1号 日本電気株式  
会社内

(74) 代理人 100071526  
弁理士 平田 忠雄

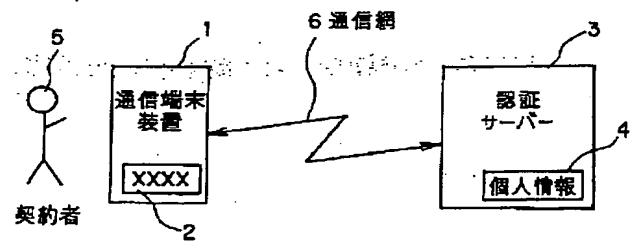
最終頁に続く

## (54) 【発明の名称】 認証システム

### (57) 【要約】

【課題】 セキュリティを確保しながら利用者を煩わせることなく、セキュリティ対策のための費用を低減することが可能な認証システムを提供する。

【解決手段】 通信端末装置 1 には製造時に付けられた固有の I D 2 を有し、通信網 6 を介して通信端末装置 1 に接続された認証サーバー 3 には、個人情報 4 が登録されている。通信端末装置 1 から接続要求があったとき、認証サーバー 3 から通信端末装置 1 に I D 2 の送信を要求する。認証サーバー 3 は、通信端末装置 1 からの I D 2 の照合により認証を行い、認証 O K のときにサービスを可能にする。



# 【特許請求の範囲】

【請求項 1】 利用者が希望するサービスの提供を通信回線又はネットワークに接続されている端末装置を介して行うに際し、前記利用者が真正であるか否かの認証を行う認証システムにおいて、前記通信回線又は前記ネットワークに認証用の個人情報が登録された認証サーバーを接続し、前記端末装置から接続要求があったとき、前記認証サーバーから前記端末装置に付けられた固有の ID の送信を要求し、受信した前記 ID の照合の可否により認証を行うことを特徴とする認証システム。

【請求項 2】 前記固有の ID は、前記端末装置の製造時に設定ならびに記憶することを特徴とする請求項 1 記載の認証システム。

【請求項 3】 前記端末装置は、携帯電話機、簡易型携帯電話機（PHS）、PDA（Personal Digital Assistant）端末装置、又はセットトップボックスであることを特徴とする請求項 1 記載の認証システム。

【請求項 4】 前記固有の ID は、前記端末装置に着脱可能な IC カードに設けられていることを特徴とする請求項 1 記載の認証システム。

【請求項 5】 前記認証サーバーは、前記端末装置からのパスワードの入力を認証条件の 1 つにすることを特徴とする請求項 1 記載の認証システム。

【請求項 6】 前記認証サーバーは、前記端末装置からのアクセスを受け付ける処理、前記端末装置に前記固有の ID の送信を要求する処理、及びウェブサーバーとの通信を行う処理を担当するエージェントが接続されていることを特徴とする請求項 1 又は 5 記載の認証システム。

【請求項 7】 前記エージェントは、電子ショッピングを実行するための買物エージェントであり、前記ウェブサーバーは、商品販売店に設置されていることを特徴とする請求項 6 記載の認証システム。

## 【発明の詳細な説明】

【0001】 本発明は、認証システムに関し、特に、通信端末装置を用い、通信回線（ネットワーク）を通して電子ショッピング等を行う際の利用者の情報漏洩を防止するための認証システムに関する。

### 【0002】

【従来の技術】 従来、通信端末装置を用いた電子ショッピングは、商品購入の都度、利用者がクレジットカードの番号或いは個人情報（住所、氏名、銀行口座番号など）を通信端末装置からネットワークに接続されたホストコンピュータに通知する方式が用いられている。また、LAN（Local Area Network）などでは、ID（Identification）やパスワード（password）等の利用者識別子を設定し、利用者が適正なアクセス者であるか否かを認証している。この場合、外部の第三者による不正アクセスの防止は、情報が外部に漏れないようにするため

に必須である。この対策については、例えば、特開 2000-10927 号公報に提案がある。

【0003】 特開 2000-10927 号公報においては、予め認証装置に利用者の「利用者 PHS 番号」、「認証装置パスワード」、「リモート接続 ID」を登録しておき、利用者が「認証装置電話番号＋認証装置パスワード」による回線接続に対し、「利用者 PHS 番号」と「認証装置パスワード」を確認し、これらが合致するときに利用者の PHS 端末機に対して一時的なパスワードを発行する旨、及び利用者 PHS 端末機の通信を一旦オフにして待つてほしい旨のメッセージを通知する。認証装置は利用者に対して一時的なパスワードを発行し、利用者の PHS 端末機に文字メッセージで表示させる。利用者は、一時的なパスワードを用いてパーソナルコンピュータ（PC）とリモート接続装置を接続することにより、ネットワークサービスを受けることが可能になる。

### 【0004】

【発明が解決しようとする課題】 しかし、従来の認証システムによれば、利用者がクレジットカード番号或いは個人情報を入力して利用者の識別を行った場合、クレジットカード番号や個人情報のなりすましが可能であり、セキュリティ上で問題が発生する可能性がある。また、利用者は情報の入力操作を強いられるという面倒がある。

【0005】 また、特開 2000-10927 号公報によれば、PHS 端末機を所持していなければ一時的なパスワードを取得できず、また、所持していても回線接続及び一時的なパスワードの入手作業が要求され、利用者にとっては煩わしい。

【0006】 したがって、本発明の目的は、セキュリティを確保しながら利用者を煩わせることなく、セキュリティ対策のための費用を低減することが可能な認証システムを提供することにある。

### 【0007】

【課題を解決するための手段】 本発明は、上記の目的を達成するため、利用者が希望するサービスの提供を通信回線又はネットワークに接続されている端末装置を介して行うに際し、前記利用者が真正であるか否かの認証を行う認証システムにおいて、前記通信回線又は前記ネットワークに認証用の個人情報が登録された認証サーバーを接続し、前記端末装置から接続要求があったとき、前記認証サーバーから前記端末装置に付けられた固有の ID の送信を要求し、受信した前記 ID の照合の可否により認証を行うことを特徴とする認証システムを提供する。

【0008】 このシステムによれば、端末装置に固有の ID と個人情報をサーバ側でデータベース化しておき、利用者が端末装置を接続した際、サーバ側から端末装置に ID を送信するように要求し、この ID の照合結果に

10

20

30

40

50

基づいて認証を実施する。したがって、利用者による認証のための入力操作を不要にできるので、個人情報等が第三者に知られるのを防止できる（セキュリティを確保できる）。また、入力操作を要求されることがないので、利用者を煩わせることがない。さらに、一時的なパスワードを発行する必要がないので、セキュリティ対策のための費用を低減することができる。

#### 【0009】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて説明する。

【第1の実施の形態】図1は本発明の認証システムを示す。1台毎に固有のID2が設定された通信端末装置1には、通信網6を介して認証サーバー3が接続されている。認証サーバー3にはID2が登録されており、さらにID2に関連付けられた個人情報4が格納されている。ID2は、製造メーカーにおいて製造時に付けられる複数桁の数字、又は数字と英字の組み合わせ等による固有のもの（製品シリアルナンバーとは異なる）で、管理者等が再設定や変更を行うことは不可能であり、同じ内容により他の通信端末装置に再使用され得ない固定されたものである。したがって、極めて識別度及び安全性の高いIDが得られる。このID2は、例えば、電子ショッピングに加入する際、管理者側に設置された専用の入力機器により読み出され、個人情報4と共に認証サーバー3に記憶される。個人情報4には、住所、氏名、銀行口座番号、信用情報等が用いられる。この個人情報4によって、通信端末装置1を用いて行われる通信サービスの契約者5が特定される。ID2と個人情報4が対応しているため、ID2から個人情報4が検索される。

【0010】通信端末装置1には、J A V A（ジャバ）仮想マシン（Java Virtual Machine）の機能を備えたものを用いる。J A V A仮想マシンは、米国のSun Microsystems社によって開発されたプログラミング言語であるJ A V Aを用いて構築されたマシンであり、Windows（登録商標）やUnix等のOS上で動作する。このような通信端末装置1として、携帯電話機、簡易型携帯電話機（PHS：Personal Handyphone System）、通信機能を備えたPDA（Personal Digital Assistant）装置、セットトップボックス（STB）等があるが、上記したように、製造段階で固有のID2が設けられていることが条件になる。

【0011】図1の構成において、認証サーバー3には、予め契約者5の個人情報4が登録されている。契約者5は、通信端末装置1を認証サーバー3に接続したいとき、認証サーバー3の呼び出しを行う。この呼び出しに対し、認証サーバー3は通信端末装置1に対してID2の送信を要求する。通信端末装置1は、認証サーバー3の要求に応じてID2を認証サーバー3へ送出する。認証サーバー3は、取得したID2が認証サーバー3に登録されているIDの中に一致するものがあるか否かを

照合する。照合できた場合、一致したID2に対応した個人情報4を用いて電子ショッピングの処理を実行する。

【0012】このように、通信端末装置1に個別に設定された固有のID2を用いて認証を行うことにより、個人情報を通信端末装置1からキー入力する必要がなくなるので、個人情報のセキュリティを確保することができる。また、個人情報を入力する必要が無いので、煩わしさを感じさせることもない。

10 【0013】〔第2の実施の形態〕上記したように、本発明は、通信端末装置1毎に設けられているIDを用いて一義的に認証を行っているため、通信端末装置1が盗難等により他人の手に渡ってしまった場合、第三者に利用されてしまう恐れがある。そこで、第2の実施の形態では、パスワードの入力を義務付けるものとする。このパスワードは、個人情報として予め登録したものを用いる。

【0014】図2は本発明による認証システムの実施例を示す。本実施例は、電子ショッピングを行うためのネットワークシステムの一例を示す。図2においては、図1に示したと同一の構成又は機能を有するものには、同一引用数字を用いている。また、図1の通信端末装置1として、携帯電話機、PHSに代表される携帯端末装置10を用いている。携帯端末装置10は、上記したように、内部に通信端末固有のID2を有しており、通信網6の加入者（契約者）の端末の位置付けにある。携帯端末装置10を使った通信サービスの契約者が契約者5である。通信網6には、認証サーバー3が接続された買物エージェント（agent）8と各商品販売店に設置されたWeb（ウェブ）サーバー（Web server）7が接続されている。認証サーバー3には、認証を行うための個人情報（住所、氏名、銀行口座番号、信用情報等）4が格納されており、一種のデータベースとして機能している。買物エージェント8は、電子ショッピングの要求を受けると起動し、内蔵する知識ベースに基づいて電子ショッピングに関する様々な処理を自律的に実行する機能を備えている。

40 【0015】図3は図2のシステムの動作を示す。また、図4は買物エージェント及び認証サーバーにおける処理を示す。図3及び図4を用いて、図2の構成の動作について説明する。以下において、図中のSはステップを表している。契約者5が電子ショッピングを行う場合、携帯端末装置10を用い、通信網6を介して買物エージェント8に接続する（S101、S201）。買物エージェント8は、携帯端末装置10の識別を行うため、J A V Aアプレット（J A V A言語をベースにして記述され、ブラウザ内で動作するプログラム）を用いて携帯端末装置10にID2の送信要求を行う（S102、S202）。この要求に対し、携帯端末装置10はID2を買物エージェント8に送信する（S103）。

買物エージェント8は、ID2を受信すると(S203)、これを認証サーバー3に送る。認証サーバー3は、ID2と事前に登録されている個人情報4により認証を行い(S104、S204)、認証が成立(S205)したときにはWebサーバー7に通知する(S105、S206)。

【0016】買物エージェント8からのID2の送信要求に対し、所定時間が経過してもID2が送られてこなかった場合、及び、認証サーバー3による認証が不成立のときには、通信を拒絶する処理を実行する(S106、S208)。認証の成立時、Webサーバー7は、通信網6及び買物エージェント8を通して(S107)、携帯端末装置10との接続を行い(S108)、携帯端末装置10とWebサーバー7の相互間で通信が行われる(S109、S110)。契約者5はWebサーバー7との間で必要な手続きを行えば、所望の商品を購入することができる。

【0017】以上のように、本発明の実施例によれば、携帯端末装置10に個別に設定された固有のID2を用いて認証を行うことにより、個人情報を携帯端末装置10からキー入力する必要がなくなるため、個人情報のセキュリティを確保することができる。また、個人情報を入力する必要が無いため、煩わしさがなくなる。

【0018】また、携帯端末装置10のID2として、携帯端末装置10の内部にIDが記憶されている形態のほか、ICカードにID2を記憶させておき、このICカードを携帯端末装置10に組み込む構成にしてもよい。さらに、上記実施の形態においては、電子ショッピングについて説明したが、本発明は電子ショッピングに限定されるものではなく、不特定多数の人が利用するインターネットや電話回線等を用い、その際に個人情報が取り扱われる全ての通信(インターネット通販、電子商

取引等)に適用可能である。

#### 【0019】

【発明の効果】以上説明した通り、本発明の認証システムによれば、端末装置に固有のIDと個人情報をサーバー側でデータベース化しておき、利用者が端末装置を接続した際、サーバー側から端末装置にIDを送信するように要求し、このIDの照合結果に基づいて認証を行うようにしたので、利用者による認証のための入力操作が不要になり、個人情報等を第三者に知られるのを防止できる結果、セキュリティの確保が可能になる。また、入力操作を強いることがないので、利用者を煩わせることがない。さらに、一時的なパスワードを発行する必要がないので、セキュリティ対策のための費用を低減することができる。

#### 【図面の簡単な説明】

【図1】本発明の認証システムを示すブロック図である。

【図2】本発明による認証システムの実施例を示すブロック図である。

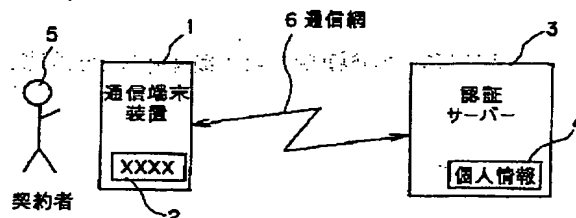
【図3】図2のシステムの動作を示すタイミングチャートである。

【図4】買物エージェント及び認証サーバーにおける処理を示すフローチャートである。

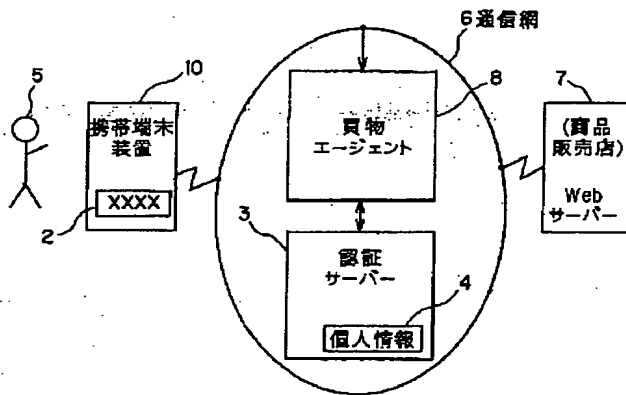
#### 【符号の説明】

- 1 通信端末装置
- 2 ID
- 3 認証サーバー
- 4 個人情報
- 6 通信網
- 7 Webサーバー
- 8 買物エージェント
- 10 携帯端末装置

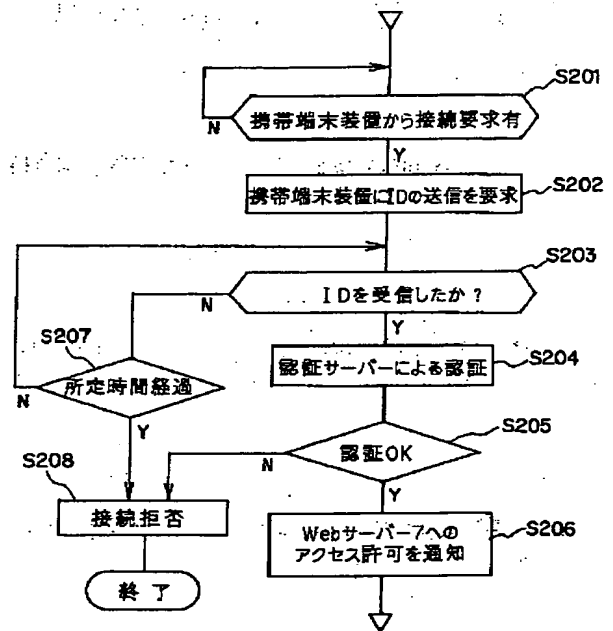
【図1】



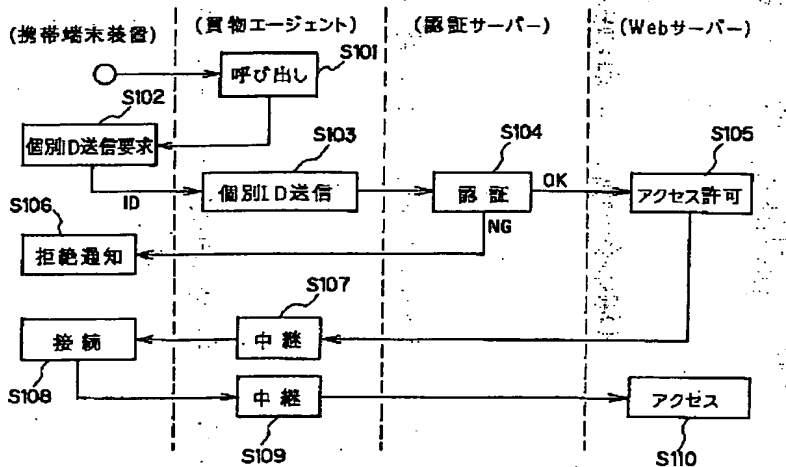
【図2】



【図4】



【図3】



フロントページの続き

(51) Int. Cl. 7

H 0 4 L 9/32

識別記号

F I

H 0 4 L 9/00

テーマコード\* (参考)

6 7 3 A

6 7 3 B

6 7 3 E

(72)発明者 佐藤 裕和  
東京都港区芝五丁目7番1号 日本電気株  
式会社内  
(72)発明者 沼崎 武  
東京都港区芝五丁目7番1号 日本電気株  
式会社内

(72)発明者 田邊 泰祐  
東京都港区芝五丁目7番1号 日本電気株  
式会社内  
Fターム(参考) 5B035 AA13 CA29  
5B058 KA12 KA33  
5B085 AE03 AE04 AE12 AE23 BG07  
5J104 AA07 KA01 KA02 MA02 NA05  
NA35 NA36 NA38 PA02 PA07